

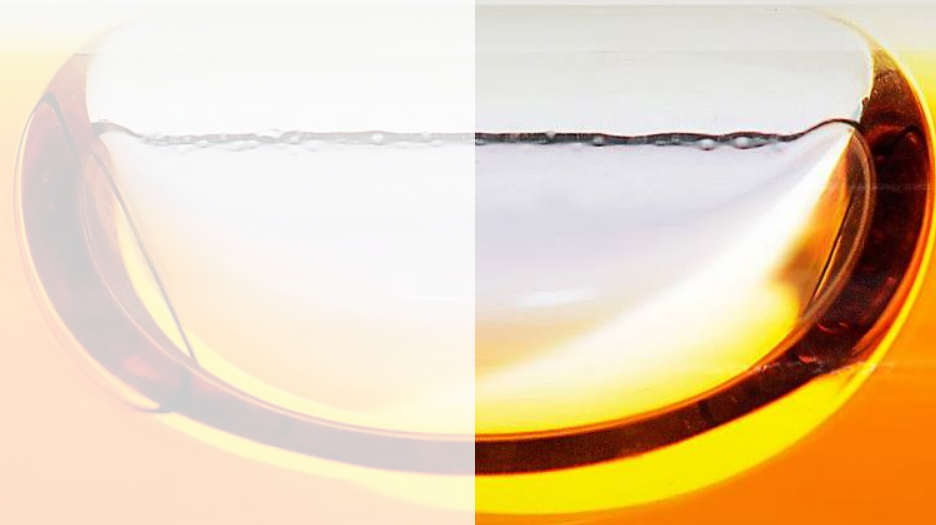


# Microsoft Entra Join and Intune, beyond the basics

Jason Sandys

Principal Product Manager Architect, Microsoft

# Level Set



# Cloud native

**Cloud-na•tive** [kloud]-['nādiv].

Endpoints or devices that can be deployed from anywhere. They receive their applications and configurations dynamically from the cloud and can be easily reset or restored.

Cloud-native endpoints are Windows devices that are deployed using Windows Autopilot, joined to Microsoft Entra ID (Entra joined), and are automatically enrolled into Microsoft Intune.

# Provisioning and enrollment recommendations

## Existing Windows endpoints

Enroll into co-management and connect to cloud identity via Entra hybrid join.



## New Windows endpoints

Provision using Autopilot user-driven mode into Intune and Entra joined (cloud-native)



# **Hybrid Entra joined and Co- Management**

These are possible  
stepping-stones to  
cloud-native.

These are **not** end  
states or goals.




# Get Started

Today (not tomorrow)



# Hybrid join and co-manage existing devices

- + Business as usual while getting immediate cloud value
- + Move management workloads to Intune 

Compliance

Application


Windows Update

} No-ops

[Configure Microsoft Entra hybrid join | Microsoft Learn](#)

[Enroll a Windows device automatically using Group Policy - Windows Client Management | Microsoft Learn](#)


# Applications

- + Win32 apps in Intune are flexible and capable  
Enterprise App Management (GA expected in Feb '24) 



# Group Policy

## Rationalize


Rationalize, don't migrate 

- Use Group Policy Analytics
- There will always be a delta, but realistically, it's small
- Use the built-in security baselines as a starting point

## Define and implement

Define and implement business requirements

## Assign and target

Assign and target policies from one authority only 

- Co-management is unrelated to Group Policy
- Do not use MDMWinsOverGPO

# Proof of Concept Now

1

Set up Autopilot

- Do not use Entra hybrid joined with Autopilot

2

Start with a minimal viable set of security policies

3

Test and focus on user scenarios including separate user personas and roles

4

Simplify

- Shift admin and management paradigm from “can” to “should”
- Empower and unlock users

[Tutorial-Get started with cloud-native Windows endpoints - Microsoft Intune | Microsoft Learn](#)  
[Success with remote Windows Autopilot and hybrid Azure Active Directory join - Microsoft Community Hub](#)

# Identify On-prem Dependencies



**Authentication on an Entra joined device to on-prem services and apps just works for the vast majority of cases**



**Internal processes, third party tools, Active Directory, DNS, NPS, on-prem only thinking**



**Use trial-and-error, decibel test, corporate knowledge during user-based POCs**

# Important Callouts

The only [Microsoft] supported process to move an existing, hybrid Entra joined Windows endpoint to Entra joined is to reset/reimage/reinstall it and re-deploy as a new device.

Entra ID and Intune are key components of Zero-trust

Implement because you “should” based on identified business requirements, not perception or because you “can”.

Test, Test, and Test some more.

Moving to cloud-native is not an overnight, all or nothing proposition. Rollout using stages, phases, rings (whatever you want to call them) based on whatever criteria makes sense in your org.





# **Engineering Reality**

Cloud-centric scenarios and cloud-native functionality is what nearly all of our engineering efforts are dedicated to and focused on. Many common challenges in the modern workplace are addressed by this approach which is based on collective customer sentiment and engagement.



# Links

- + <https://aka.ms/cloudnativeendpoints>
- + <https://aka.ms/EntraJoin-WhichOption>
- + <https://learn.microsoft.com/en-us/entra/identity/devices/how-to-hybrid-join>
- + <https://learn.microsoft.com/en-us/windows/client-management/enroll-a-windows-10-device-automatically-using-group-policy>
- + <https://learn.microsoft.com/en-us/mem/solutions/cloud-native-endpoints/cloud-native-windows-endpoints>
- + <https://techcommunity.microsoft.com/t5/intune-customer-success/success-with-remote-windows-autopilot-and-hybrid-azure-active/ba-p/2749353>
- + <https://learn.microsoft.com/en-us/entra/identity/devices/device-sso-to-on-premises-resources>

